



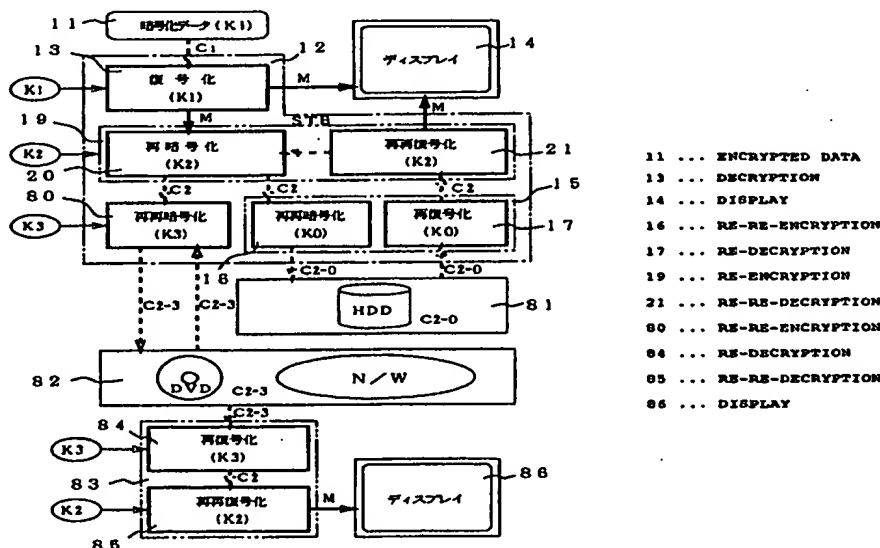
PCT

特許協力条約に基づいて公開された国際出願

<p>(51) 国際特許分類7 H04L 9/14, G11B 20/10, H04N 7/167, G06F 17/60</p>	<p>A1</p>	<p>(11) 国際公開番号 WO00/22777</p> <p>(43) 国際公開日 2000年4月20日(20.04.00)</p>
<p>(21) 国際出願番号 PCT/JP99/05704</p> <p>(22) 国際出願日 1999年10月15日(15.10.99)</p> <p>(30) 優先権データ 特願平10/309418 1998年10月15日(15.10.98)</p> <p>(71) 出願人 (米国を除くすべての指定国について) 三菱商事株式会社(MITSUBISHI CORPORATION)[JP/JP] 〒100-8086 東京都千代田区丸の内二丁目6番3号 Tokyo, (JP)</p> <p>(72) 発明者 ; および</p> <p>(75) 発明者 / 出願人 (米国についてのみ) 斉藤 誠(SAITO, Makoto)[JP/JP] 〒206-0012 東京都多摩市貝取2-12-6-104 Tokyo, (JP)</p> <p>(74) 代理人 南條真一郎(NANJO, Shin-ichiro) 〒101-0053 東京都千代田区神田美土代町7 南條特許事務所 Tokyo, (JP)</p>		<p>(81) 指定国 AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), ARIPO特許 (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM)</p> <p>添付公開書類 国際調査報告書</p>

(54)Title: METHOD AND DEVICE FOR PROTECTING DIGITAL DATA BY DOUBLE RE-ENCRYPTION

(54)発明の名称 2重再暗号化によりデジタルデータを保護する方法及び装置



(57) Abstract

A method and a device capable of protecting digital data reliably. Digital data are doubly re-encrypted by using a fixed key and a variable key. The order of using the encrypting keys is first the variable key and then the fixed key, or first the fixed key and then the variable key. The working examples are exemplified by one using a software, one using a hardware and one using a combination of a software and a hardware. The hardware can use a fixed key which has been developed for digital video. The software performs encryption/decryption in a region other than a kernel portion which cannot be used by the user so as to keep the safety of the program and the key used. Specifically, the encryption/decryption are performed by a filter driver in an I/O manager, a device driver serving as a disk driver/net driver and an RTOS utilizing an HAL. Either or both of two filter drivers on both sides of a file system driver can be used.

明 細 書

2 重再暗号化によりデジタルデータを保護する方法及び装置

技術分野

本発明は、デジタルコンテンツの管理、特に著作権主張がされたデジタルコンテンツの著作権管理、デジタルコンテンツの秘密保護、を行うことによりデジタルコンテンツの流通を図りデジタルコンテンツ経済を実現する方法及び装置に関する。

背景技術

従来広く普及しているアナログコンテンツは保存、複写、加工、転送をする毎に品質が劣化するために、これらの作業によって生じる著作権の処理は大きな問題とはならなかった。しかし、デジタルコンテンツは保存、複写、加工、転送を繰り返して行っても品質劣化が生じないため、これらの作業によって生じる著作権の処理は大きな問題である。

デジタル映像・音声等のデジタルデータは放送、DVD等によって有料でユーザに供給されることが多く、その場合に無料視聴を防止するために暗号化されて供給される。暗号化されて供給されたデジタルデータは何等かの手段によって供給された暗号鍵を用いて復号され、視聴される。復号されたデジタルデータは保存、複写あるいは転送を行っても品質が劣化することはないため、ユーザによって保存、複写あるいは転送が行われた場合には二次的な無料視聴が行われることになり、復号されたデジタルデータコンテンツの再度の利用はコンテンツ提供者の利益に反するため、再度の利用すなわち保存、複写あるいは転送の二次利用を禁止することでシステム及び機器の開発が進められてきた。

しかし、二次利用を禁止することは利用者にとってはデジタルデータコンテンツの利用が魅力の乏しいものとなり、デジタルデータコンテンツの普及を阻害す

ムは、デジタル映像コンテンツのリアルタイム送信も含むデータベースシステムにおけるデジタルコンテンツの表示（音声化を含む）、保存、複写、加工、転送における著作権の管理を行うために、利用を許可する鍵の他に、著作権を管理するためのプログラム及び著作権情報を用いる。

この著作権管理プログラムは、申し込みあるいは許可内容に反する利用が行われないように監視し管理を行う。

また、この特開平 7-271865 号 (EP0677949A2, USSN08/416037) には、デジタルコンテンツが暗号化された状態でデータベースから供給され、著作権管理プログラムによって表示・加工のときにのみ復号化され、保存、コピー、転送は再び暗号化された状態で行うことが記載されている。さらに、著作権管理プログラム自体を暗号化し、許可鍵で著作権管理プログラムを復号化し、復号化された著作権管理プログラムが著作権データの復号化及び暗号化を行うこと、データの保存及び表示以外の利用が行われた場合には操作者についての情報を含む著作権情報を原著作権情報に加えて履歴として保存することも記載されている。

特開平 8-287014 号 (USP5867579, EP0715241A2) において著作権管理を行うためのボード、PCMCIA カードあるいは IC カード、IC の形態を有する復号／再暗号化用装置及び暗号鍵の寄託システムを提案した。またこの出願では著作権管理方法のテレビジョン会議及び電子商取引への応用についても言及した。

なお、USP 5805706 にも IC の形態を有する復号／再暗号化用装置が記載されている。

特開平 8-272745 号 (USP5646999, EP0709760) において複数データを利用した加工データの原データ著作権及び加工データ著作権の保護を秘密鍵（共通鍵）方式と公開鍵方式を組み合わせる加工プログラムへのデジタル署名で申込みの正当性を確認することによって行うシステムを提案した。

特開平 8-288940 号 (USP5740246, EP0719045A2) において、データベース、

$$M = D(C, K)$$

という式で表現する。

また、復号化データMの再暗号化／再復号化を繰り返す場合の再暗号化は、

$$\forall i: C_i = E(D(C_{i-1}, K_{i-1}), K_i) \quad \text{但し } i \text{ は正の整数}$$

という式で表現し、再復号化は、

$$\exists: M = D(E(C_{i-1}, K_{i-1}), K_i)$$

という式で表現する。

第1図により、従来提案されているセットトップボックス(STB)の構成及びこのセットトップボックスで行われているデジタルデータ保護方法を説明する。

なお、暗号化／復号化と直接には関係がない周辺回路、例えば増幅ユニット、圧縮／伸長ユニットはこの説明において省略されている。

この図において、1はデジタル地上波放送、デジタルCATV放送、デジタル衛星放送等の放送手段、インターネット等のネットワーク手段あるいはDVD、CD等のデジタル保存媒体により供給されるデジタルデータであり、不正利用を防止するために第1可変鍵K1を用いて暗号化されて、

$$C1 = E(M, K1)$$

セットトップボックス2に供給される。

暗号化デジタルデータC1を供給されたセットトップボックス2では、暗号化デジタルデータC1と同じ経路あるいは暗号化デジタルデータC1と異なる経路により鍵センターから入手した第1可変鍵K1を用い、復号化ユニット3において暗号化デジタルデータC1を復号し、

$$M = D(C1, K1)$$

得られた復号化データMがディスプレイ装置4等に出力される。

復号化データMがデジタルビデオディスクRAM(DVD)あるいはハードディスク等の媒体に保存される場合、又はネットワークを経由して外部に転送され

図面の簡単な説明

第1図は、従来提案されているセットトップボックスの概要構成説明図である。

第2図は、セットトップボックスに適用した第1実施例の概要構成説明図である。

第3図は、セットトップボックスに適用した第2実施例の概要構成説明図である。

第4図は、パーソナルコンピュータを用いた装置に適用した第3実施例の概要構成説明図である。

第5図は、パーソナルコンピュータを用いた装置に適用した第4実施例の概要構成説明図である。

第6図は、第4実施例の詳細な説明図である。

第7図は、パーソナルコンピュータを用いた装置に適用した第5実施例の概要構成説明図である。

第8図は、第1実施例の変形である第6実施例のセットトップボックスの概要構成説明図である。

第9図は、第6実施例の変形である第7実施例のセットトップボックスの概要構成説明図である。

第10図は、パーソナルコンピュータを用いた第8実施例の概要構成説明図である。

第11図は、第8実施例の詳細な説明図である。

第12図は、著作権管理装置の実施例説明図である。

第13図は、著作権管理装置の他の実施例説明図である。

第14図は、著作権管理装置のさらに他の実施例説明図である。

発明を実施するための最良の形態

本願発明の実施例を説明する。

第2図により本発明を適用した第1実施例であるセットトップボックス（STB）の構成及びこのセットトップボックスで行われているデジタルデータ保護方法を説明する。

なお、この実施例のセットトップボックスにおいても第1図に示された従来例のセットトップボックスの場合と同様に、暗号化／復号化と直接には関係がない周辺回路、例えば増幅ユニット、圧縮／伸長ユニット及び外部装置へのインターフェース装置の説明は省略されている。

この実施例が第1図に示された従来提案されているセットトップボックスと異なる点は、復号化ユニット13と固定鍵K0を用いて暗号化／復号化を行う固定鍵方式暗号化／復号化ユニット15の間に第2可変鍵K2を用いて暗号化／復号化を行う可変鍵方式暗号化／復号化ユニット19が挿入されている点である。この第2可変鍵K2は外部から供給される場合とセットトップボックス内で生成される場合がある。

この図において、11はデジタル地上波放送、デジタルCATV放送、デジタル衛星放送等の放送手段、インターネット等のネットワーク手段あるいはDVD、CD等のデジタル保存媒体により供給されるデジタルデータであり、不正利用を防止するために第1可変鍵K1を用いて暗号化されて、

$$C1 = E(M, K1)$$

セットトップボックス12に供給される。

暗号化デジタルデータC1を供給されたセットトップボックス12では、暗号化デジタルデータC1と同じ経路あるいは暗号化デジタルデータC1と異なる経路により鍵センタから入手した第1可変鍵K1を用い、復号化ユニット13において暗号化デジタルデータC1を復号し、

$$M = D(C1, K1)$$

され、可変鍵K2及び固定鍵K0を用いて再暗号化されたものが再保存されるように構成されることもある。

このように、固定鍵K0を用いて再暗号化する前に第2可変鍵K2を用いて再暗号化する構成により、万一固定鍵K0が知られてしまった場合でもデータは第2可変鍵K2でも暗号化されているため、さらに第2可変鍵K2を見いだして暗号化データの解読を行うことは極めて困難になる。

また、第2可変鍵K2は初めに再暗号化に使用され、固定鍵K0が再再暗号化及び再復号化に使用された後に、再再復号化に使用されるため、第2可変鍵K2の安全性が高く、かつ初めに使用されるため、暗号化データを最も強力に支配することになる。

この実施例においては、暗号化ユニット20及び復号化ユニット21が可変鍵方式暗号化／復号化ユニット19に含まれ、暗号化ユニット16及び暗号化ユニット17が固定鍵方式暗号化／復号化ユニット15に含まれたものについて説明したが、これらのユニット16、17、20、21が分離して設けられても良いことは当然のことである。

なお、このような動作はセットトップボックス12内にCPUとシステムバスを有するコンピュータ構成を設けることにより容易に実現することができる。

第3図により本発明を適用した第2実施例であるセットトップボックス(STB)の他の構成及びこのセットトップボックスで行われているデジタルデータ保護方法を説明する。

なお、この第2実施例のセットトップボックスにおいても第1図に示された従来例のセットトップボックスの場合と同様に、暗号化／復号化と直接には関係がない周辺回路、例えば増幅ユニット、圧縮／伸長ユニットの説明は省略されている。

この第2実施例のセットトップボックスが第2図に示された第1実施例のセットトップボックスと異なる点は、固定鍵K0を用いて暗号化／復号化を行う固定鍵

さらに第2可変鍵K2を用い、可変鍵方式暗号化／復号化ユニット39の暗号化ユニット40において復号化データMが再再暗号化され、

$$\begin{aligned}\forall 0-2: C0-2 &= E(C0, K2) \\ &= E(E(D(C1, K1), K0), K2)\end{aligned}$$

再再暗号化データC0-2として外部装置38に保存あるいは転送される。

再再暗号化データC0-2が再利用される場合には、外部装置38の保存媒体から読み出されたあるいはネットワークを経由して転送された再暗号化データC0-2が可変鍵方式暗号化／復号化ユニット39の復号化ユニット41において第2可変鍵K2を用いて再復号化され、

$$\begin{aligned}\exists 0: C0 &= E(C0-2, K2) \\ &= D(E(E(D(C1, K1), K0), K2)\end{aligned}$$

さらに固定鍵方式暗号化／復号化ユニット35の復号化ユニット37において再復号化データC0が固定鍵K0を用いて再再復号化され、

$$\begin{aligned}\exists: M &= D(C0, K0) \\ &= D(E(D(C1, K1), K0)\end{aligned}$$

得られた復号化データMがディスプレイ装置34等に出力される。

この場合安全を期するために、図中に破線で示した経路により再暗号化データC0-2が保存媒体から読み出される時に保存媒体中の再再暗号化データC0-2が消去され、固定鍵K0及び第2可変鍵K2を用いて再暗号化されたものが再保存されるように構成されることもある。

このように、固定鍵K0を用いて再暗号化する前に第2可変鍵K0を用いて再暗号化する構成により、もし固定鍵K0が知られてしまった場合でもデータは第2可変鍵K0でも暗号化されているため、さらに第2可変鍵K0を見いだして暗号化データの解読を行うことは極めて困難になる。

また、この構成は第1図に示された従来提案されているセットトップボックスの固定鍵方式暗号化／復号化ユニット35にさらに可変鍵方式暗号化／復号化ユ

用者からの要求性能の向上に伴い、コンピュータの全体の動作を統括するオペレーティングシステムも機能向上が要求され、以前と比較してオペレーティングシステムの規模が肥大している。

このような肥大したオペレーティングシステムはオペレーティングシステム自身がその保存場所であるハードディスクの大きなスペースを占領するため、ユーザが必要とするアプリケーションプログラムあるいはデータを保存するスペースが不足がちになり、コンピュータの使い勝手が悪くなるという事態が発生する。

このような事態に対処するために、最新のオペレーティングシステムはカーネルから他のオペレーティングシステムのエミュレーション及び画面描画を行う環境サブシステムと、セキュリティサブシステム等の中核サブシステムとをユーザに依存する部分であるサブシステム(Sub system)として取り除き、ハードウェアの相異を吸収するHAL (Hardware abstraction Layer), スケジューリング機能, 割り込み機能, I/O管理機能等の基本的部分をマイクロカーネル(Micro kernel)とし、サブシステムとマイクロカーネルの間にシステムサービスAPI (Application Programming Interface)を介在させてオペレーティングシステムを構成している。

このようにすることにより、機能変更あるいは追加によるオペレーティングシステムの拡張性が向上するとともに、用途に対応する移植が容易になる。

また、マイクロカーネルの要素をネットワーク化された複数のコンピュータに分散配置することにより、分散オペレーティングシステムを実現することが容易になる。

コンピュータはデスクトップ型あるいはノート型に代表されるパーソナルコンピュータ以外に、コンピュータ周辺機器、各種制御装置、通信機等に使用されている。その場合、各々の装置に適合するエンベデッド用の専用オペレーティングシステムとしてマン・マシン・インターフェースが重視される汎用のパーソナルコンピュータ用オペレーティングシステムと異なり、実行の早さが重視されるリ

つのプロセス中にはシステム資源を共有する一つ以上のスレッドが存在することになる。

マルチタスク方式で処理される各タスクには優先順位(Priority Spectrum)があり、一般的には32の段階に分けられる。この場合、割り込みを行わない通常のタスクは0-15段階に分けられるダイナミッククラス(Dynamic Classes)に区分され、割り込みを行うタスクは16-31段階に分けられるリアルタイムクラス(Real-Time Classes)に区分される。

割り込み処理はタイムスライスと呼ばれる割り込み可能時間(通常10ms)を単位として行われ通常の割り込みは10msのタイムスライスで行われている。

このような状況において、最近リアルタイムスライスと呼ばれる割り込み可能時間が100 μ sであるタイムスライスが提案されたが、このリアルタイムスライスを利用すれば従来の10msの割り込みよりも優先して割り込みが可能である。

第4図に示された第3実施例では、ソフトウェアにより行われるコンピュータによる可変鍵方式暗号化/復号化処理及び暗号鍵の管理は、HALにおいてリアルタイムOSにより行われる。

この図において51はコンピュータ内のオペレーティングシステム、56はコンピュータからの出力を表示するディスプレイ装置、57は固定鍵方式暗号化/復号化ユニット、58はデジタルビデオディスク(DVD)RAMあるいはハードディスク等のデータ保存媒体、又はネットワーク等のデータ転送装置である。

オペレーティングシステム51はユーザ領域であるオペレーティングシステムサービス部52、システムサービスAPI部53、非ユーザ領域であるカーネル54部及びHAL55から構成され、システムサービスAPI部53はオペレーティングシステムサービス部52とカーネル部54の間に配置されて、オペレーティングシステムサービス部52とカーネル部54を仲介する役割を果たしており、HAL55はオペレーティングシステム50の最下層に配置され、ソフトウェアから見たハードウェアハードウェアの相異を吸収する役割を担っている。

オペレーティングシステムサービス部52はアプリケーション59、サブシス

由して外部に転送される場合は、第2可変鍵K2を用い、HAL 55において復号化データMが強制的に再暗号化され、

$$\begin{aligned}\forall 2: C2 &= E(M, K2) \\ &= E(D(C1, K1), K2)\end{aligned}$$

さらに固定鍵方式暗号化／復号化装置57において再暗号化データC2が固定鍵K0を用いて再再暗号化され、

$$\begin{aligned}\forall 2-0: C2-0 &= E(C2, K0) \\ &= E(E(D(C1, K1), K2), K0)\end{aligned}$$

再再暗号化データC2-0として外部装置58に保存あるいは転送される。この可変鍵K2は外部から供給される場合とセットトップボックス内で生成される場合がある。

再再暗号化データC2-0が利用される場合には、保存媒体から読み出されたあるいはネットワークを経由して転送された再暗号化データC2-0が固定鍵方式暗号化／復号化装置57において固定鍵K0を用いて再復号化され、

$$\begin{aligned}\exists 2: C2 &= E(C2-0, K0) \\ &= D(E(E(D(C1, K1), K2), K0)\end{aligned}$$

さらに可変鍵方式暗号化／復号化機能を有するHAL 55において再復号化データC2が第2可変鍵K2を用いて復号化され、

$$\begin{aligned}\exists: M &= D(C2, K2) \\ &= D(E(D(C1, K1), K2)\end{aligned}$$

得られた復号化データMがディスプレイ装置56等に出力される。

リアルタイムOSは他の全てのタスクに優先して実行され、この第3実施例においてはリアルタイムOSがオペレーティングシステムのハードウェアとの接点であるHALにおいて実行されるから、デジタルデータの再暗号化が確実に行われ、復号化データMをそのまま外部装置58に保存あるいは転送することは不可能となる。また、固定鍵K0を用いて再暗号化する前に第2可変鍵K2を用いて再暗号化することにより、もし固定鍵K0が知られてしまった場合でもデータは第2

能を有するモジュールをフィルタドライバ66Aあるいはフィルタドライバ66BとしてI/O管理モジュールに挿入する。

第2図の第1実施例の場合と同様に、デジタル地上波放送、デジタルCATV放送、デジタル衛星放送等の放送手段、インターネット等のネットワーク手段あるいはDVD、CD等のデジタル保存媒体により供給されるデジタルデータは、不正利用を防止するために第1可変鍵K1を用いて暗号化されて、

$$C1 = E(M, K1)$$

供給され、供給された暗号化デジタルデータC1は暗号化デジタルデータC1と同じ経路あるいは暗号化デジタルデータC1と異なる経路により鍵センタから提供された第1可変鍵K1を用いてオペレーティングシステムサービス部52により復号され、

$$M = D(C1, K1)$$

復号化データMがディスプレイ装置56等に出力される。

著作権主張がなされた復号化データMがデジタルビデオディスク(DVD)RAMあるいはハードディスク等の媒体に保存される場合、又はネットワークを経由して外部に転送される場合は、第2可変鍵K2を用い、フィルタドライバ66Aあるいは66Bにおいて復号化データMが強制的に再暗号化され、

$$\forall 2: C2 = E(M, K2) = E(D(C1, K1), K2)$$

さらに内蔵固定鍵方式暗号化/復号化装置57において再暗号化データC2が固定鍵K0を用いて再再暗号化され、

$$\forall 2-0: C2-0 = E(C2, K0)$$

$$= E(E(D(C1, K1), K2), K0)$$

再再暗号化データC2-0として外部装置58に保存あるいは転送される。この可変鍵K2は外部から供給される場合とセットトップボックス内で生成される場合がある。

再再暗号化データC2-0が再利用される場合には、保存媒体から読み出されたあ

ライバ71が配置されており、その最下層に位置するデバイスドライバ71でも可変鍵方式暗号化／復号化処理及び鍵管理を行うことができる。

第2図の第1実施例の場合と同様に、デジタル地上波放送、デジタルCATV放送、デジタル衛星放送等の放送手段、インターネット等のネットワーク手段あるいはDVD、CD等のデジタル保存媒体により供給されるデジタルデータは、不正利用を防止するために第1可変鍵K1を用いて暗号化されて、

$$C1 = E(M, K1)$$

供給され、供給された暗号化デジタルデータC1は暗号化デジタルデータC1と同じ経路あるいは暗号化デジタルデータC1と異なる経路により鍵センタから提供された第1可変鍵K1を用いてオペレーティングシステムサービス部52により復号され、

$$M = D(C1, K1)$$

得られた復号化データMがディスプレイ装置56等に出力される。

著作権主張がなされた復号化データMがデジタルビデオディスク(DVD)RAMあるいはハードディスク等の媒体に保存される場合、又はネットワークを経由して外部に転送される場合は、第2可変鍵K2を用い、ディスクドライバ67及びネットワークドライバ68であるデバイスドライバ71において復号化データMが強制的に再暗号化され、

$$\begin{aligned} \forall 2 : C2 &= E(M, K2) \\ &= E(D(C1, K1), K2) \end{aligned}$$

さらに固定鍵方式暗号化／復号化装置57において再暗号化データC2がその固定鍵方式暗号化／復号化装置57に内蔵された固定鍵K0を用いて再再暗号化され、

$$\begin{aligned} \forall 2-0 : C2-0 &= E(C2, K0) \\ &= E(E(D(C1, K1), K2), K0) \end{aligned}$$

再再暗号化データC2-0として外部装置58に保存あるいは転送される。この第2可変鍵K2は外部から供給される場合とセットトップボックス内で生成される場合がある。

これまでに説明した実施例では第1可変鍵K1の他に第2可変鍵K2及び内蔵固定鍵K0を使用している。これから説明する実施例では加えて第3の可変鍵K3を使用することによりさらに強固にデジタルコンテンツの著作権管理を行う。

第8図により第1実施例の変形である第6実施例のセットトップボックスの構成及びこのセットトップボックスで行われているデジタルデータ保護方法を説明する。

なお、この実施例のセットトップボックスにおいても第1実施例のセットトップボックスの場合と同様に、暗号化／復号化と直接には関係がない周辺回路、例えば増幅ユニット、圧縮／伸長ユニットの説明は省略されている。

この第6実施例のセットトップボックスが第1実施例のセットトップボックスと異なる点は、復号化データMがハードディスク等のセットトップボックス内蔵あるいは専用の保存媒体81に保存される場合と外部装置82において可搬媒体であるDVD RAM等に保存又はネットワークを経由して外部に転送される場合とが区別されている点である。

そのために、内蔵固定鍵方式暗号化／復号化ユニット15の他に可変鍵方式暗号化ユニット80が設けられ、著作権主張がなされた復号化データがセットトップボックス内蔵あるいは専用の保存媒体81であるハードディスク等に保存される場合には内蔵固定鍵K0で再再暗号化されるが、可搬媒体であるDVD RAMに保存されあるいはネットワークを経由して外部に転送される場合には内蔵固定鍵K0ではなく第3可変鍵K3で再再暗号化される。

この図において、11はデジタル地上波放送、デジタルCATV放送、デジタル衛星放送等の放送手段、インターネット等のネットワーク手段あるいはDVD、CD等のデジタル保存媒体により供給されるデジタルデータであり、不正利用を防止するために第1可変鍵K1を用いて暗号化されて、

$$C1 = E(M, K1)$$

て復号化され、

$$\begin{aligned}\exists 2: C2 &= D(C2-0, K0) \\ &= D(E(E(D(C1, K1), K2), K0)) \\ &= E(E(D(C1, K1), K2))\end{aligned}$$

さらに可変鍵方式暗号化／復号化ユニット 19 の復号化ユニット 21 において再復号化データ C2 が可変鍵 K2 を用いて復号化され、

$$\begin{aligned}\exists: M &= D(C2, K2) \\ &= D(E(D(C1, K1), K2))\end{aligned}$$

復号化データ M がディスプレイ装置 14 等に出力される。

この場合安全を期するために、図中に破線で示した経路により再暗号化データ C2-0 が保存媒体 81 から読み出される時に保存媒体 81 中の再暗号化データ C2-0 が消去され、可変鍵 K2 及び内蔵固定暗号鍵 K0 を用いて再暗号化されたものが再保存されるように構成されることもある。

再暗号化データ C2 が外部装置 82 において可搬媒体である DVD-RAM に保存されあるいはネットワークを経由して外部に転送される場合には可変鍵方式暗号化ユニット 80 において、鍵センタから入手あるいはセットトップボックス 12 内で生成した第 3 可変鍵 K3 を用い、再暗号化データ C2 が再再暗号化される。

$$\begin{aligned}\forall 2-3: C2-3 &= E(C2, K3) \\ &= E(E(M, K2), K3)\end{aligned}$$

外部装置 82 を経由した再再暗号化データ C2-3 が利用される場合には、再再暗号化データ C2-3 が可変鍵方式暗号化／復号化ユニット 83 の復号化ユニット 84 において内蔵された第 3 可変鍵 K3 を用いて復号化され、

$$\begin{aligned}\exists 2: C2 &= D(C2-3, K3) \\ &= D(E(M, K2), K3) \\ &= E(M, K2)\end{aligned}$$

さらに得られた再暗号化データ C2 が可変鍵方式暗号化／復号化ユニット 83 の復

暗号化デジタルデータ C1 が供給されたセットトップボックス 12 では、鍵センタから入手した第 1 可変鍵 K1 を用い、復号化ユニット 13 において暗号化デジタルデータ C1 を復号し、

$$M = D(C1, K1)$$

得られた復号化データ M がディスプレイ装置 14 等に出力される。

著作権主張がなされた復号化データ M がハードディスク等のセットトップボックス 12 に内蔵されたあるいは専用の保存媒体 81 に保存される場合には、復号化データ M が内蔵固定鍵方式暗号化／復号化ユニット 15 において固定暗号鍵 K0 を用いて再暗号化データ C0 に再暗号化される。

$$\begin{aligned} \forall 0 : C0 &= E(M, K0) \\ &= E(D(C1, K1), K0) \end{aligned}$$

再暗号化データ C0 は、鍵センタから入手あるいはセットトップボックス 12 内で生成した第 2 可変鍵 K2 を用いて可変鍵方式暗号化／復号化ユニット 19 の暗号化ユニット 20 において再再暗号化され、

$$\begin{aligned} \forall 0-2 : C0-2 &= E(C0, K2) \\ &= E(E(M, K0), K2) \end{aligned}$$

再再暗号化データ C0-2 が保存媒体 81 等に保存される。

保存媒体 81 に保存されている再再暗号化データ C0-2 が利用される場合には、保存媒体 81 から読み出された再再暗号化データ C0-2 が第 2 可変鍵 K2 を用いて可変鍵方式暗号化／復号化ユニット 19 の復号化ユニット 21 において再復号化され、

$$\begin{aligned} \exists 0 : C0 &= D(C0-2, K2) \\ &= D(E(C0, K2), K2) \end{aligned}$$

さらに固定鍵方式暗号化／復号化ユニット 15 の復号化ユニット 17 において再復号化データ C0 が固定鍵 K0 を用いて再再復号化され、

$$\exists : M = D(C0, K0)$$

さらに得られた再再暗号化データC2が可変鍵方式暗号化／復号化ユニット83の復号化ユニット85において第3可変鍵K3を用いて復号化され、

$$\begin{aligned} \exists : M &= D(C3, K3) \\ &= D(E(M, K3), K3) \end{aligned}$$

得られた復号化データMがディスプレイ装置86等に出力される。

なお、この実施例においては可変鍵方式暗号化ユニット80において、第3可変鍵K3を用い、可変鍵方式暗号化ユニット87において、第2可変鍵K2を用いているが、この順番は逆にすることも可能である。

また、可変鍵方式暗号化ユニット87の機能を可変鍵方式暗号化／復号化ユニット19の暗号化ユニット20において行うように構成することも可能である。

さらに、暗号化ユニット16及び復号化ユニット17が固定鍵方式暗号化／復号化ユニット15に含まれ、暗号化ユニット20及び復号化ユニット21が可変鍵方式暗号化／復号化ユニット19に含まれたものについて説明したが、これらのユニット16、17、20、21が分離して設けられても良いことは当然のことである。

このような動作は、セットトップボックス12内にCPUとシステムバスを有するサブコンピュータ構成を設けることにより容易に実現することができる。

パーソナルコンピュータを用いた装置に適用した実施例の変形実施例を説明する。

第10図に示された第8実施例は第5図に示された第4実施例の変形実施例であるが、この実施例の構成中第4実施例と共通する部分の説明は省略する。

この第8実施例が第4実施例と異なる点は、復号化データMがハードディスク等のコンピュータ内蔵あるいは専用の保存媒体81に保存される場合と可搬媒体92であるDVD RAM等に保存又はネットワーク93を経由して外部に転送される場合とが区別されている点である。

さらに、再暗号化データC2がコンピュータ内蔵あるいは専用の保存媒体81に保存される場合にはハードウェア88内の暗号化／復号化ユニット89において固定鍵K0を用いて再暗号化データC2が再再暗号化され、

$$\forall 2-0: C2-0 = E(C2, K0) = E(E(D(C1, K1), K2), K0)$$

再再暗号化データC2-0としてハードディスク81等に保存される。

保存媒体81に保存された再再暗号化データC2-0が利用される場合には、保存媒体81から読み出された再暗号化データC2-0がハードウェア88内の暗号化／復号化ユニット89において固定暗号鍵K0を用いて再復号化され、

$$\exists 2: C2 = E(C2-0, K0) = D(E(E(D(C1, K1), K2), K0))$$

さらに暗号化／復号化機能を有するフィルタドライバ66において再復号化データC2が第2可変鍵K2を用いて復号化され、

$$\exists: M = D(C2, K2) = D(E(D(C1, K1), K2))$$

復号化データMがコンピュータのオペレーティングシステムによりディスプレイ装置56等に出力される等利用される。

また、再暗号化データC2がDVDRAM等の可搬媒体に保存される場合には、ハードウェアである可変鍵方式暗号化／復号化ユニット90において第2可変鍵K2を用いて再暗号化データC2が再再暗号化され、

$$\forall 2-3: C2-3 = E(C2, K3) = E(E(D(C1, K1), K2), K3)$$

再再暗号化データC2-3としてDVDRAM等の可搬媒体に保存される。

可搬媒体92に保存された再再暗号化データC2-3が利用される場合には、可搬媒体92から読み出された再暗号化データC2-3がハードウェア内の暗号化／復号化ユニット90において鍵センタから入手あるいはオペレーティングシステムサービス部52内で生成した第3可変鍵K3を用いて再復号化され、

$$\exists 2: C2 = E(C2-3, K3) = D(E(E(D(C1, K1), K2), K3))$$

さらに暗号化／復号化機能を有するフィルタドライバ66において再復号化デー

ンピュータ構成とすることにより容易に実現することができる。

第11図に示されたのは、第8実施例の可変鍵方式暗号化／復号化処理を行うフィルタドライバ66を有するI/O管理マイクロカーネルモジュール64を用いた暗号化／復号化処理の具体的な構成である。

I/O管理マイクロカーネルモジュール64は上位階層から下位階層にファイルシステムドライバ69、中間ドライバ70、デバイスドライバであるディスクドライバ67及びネットワークドライバ68が配置されており、必要に応じてファイルシステムドライバ69の上位階層あるいは中間ドライバ70とデバイスドライバとの間に可変鍵方式暗号化／復号化処理を行うフィルタドライバ66Aあるいはフィルタドライバ66Bが挿入される。

これらのフィルタドライバ66A及びフィルタドライバ66Bによって再暗号化／再復号化処理をさせることが可能であるため、この実施例においては再暗号化／再復号化処理及び暗号鍵の管理をフィルタドライバ66Aあるいはフィルタドライバ66Bに実行させる。

著作権主張がなされた復号化データMが内蔵あるいは専用のハードディスク等の保存媒体に保存される場合あるいはDVDRAM等の可搬媒体に保存される場合、又はネットワークを経由して外部に転送される場合は、鍵センタから入手あるいはI/O管理マイクロカーネルモジュール64内で生成した第2可変鍵K2を用い、フィルタドライバ66Aあるいは66Bにおいて復号化データMが再暗号化される。

$$\forall 2: C2 = E(M, K2) = E(D(C1, K1), K2)$$

さらに、再暗号化データC2がコンピュータ内蔵あるいは専用の保存媒体81に保存される場合にはハードウェア88内の暗号化／復号化ユニット89において固定鍵K0を用いて再暗号化データC2が再再暗号化され、

$$\forall 2-0: C2-0 = E(C2, K0) = E(E(D(C1, K1), K2), K0)$$

また、再暗号化データ C2 がネットワーク 93 を経由して外部に転送される場合には、暗号化／復号化ユニット 91 において第 2 可変鍵 K2 を用いて再暗号化データ C2 が再再暗号化され、

$$\forall 2-3: C2-3 = E(C2, K3) = E(E(D(C1, K1), K2), K3)$$

再再暗号化データ C2-3 としてネットワーク 93 を経由して外部に転送される。

ネットワーク 93 を経由して外部から転送された再再暗号化データ C2-3 を利用する場合には、暗号化データ C2-3 が暗号化／復号化ユニット 91 において第 3 可変鍵 K3 を用いて再復号化され、

$$\exists 2: C2 = E(C2-3, K3) = D(E(E(D(C1, K1), K2), K3)$$

さらに暗号化／復号化機能を有するフィルタドライバ 66 において再復号化データ C2 が第 2 可変鍵 K2 を用いて復号化され、

$$\exists: M = D(C2, K2) = D(E(D(C1, K1), K2)$$

復号化データ M がコンピュータのオペレーティングシステムによりディスプレイ装置 56 等に出力される等利用される。

デバイスドライバは、オペレーティングシステムを使用するコンピュータに合わせてあるいは対象となるデバイスが改良されたような場合に仕様を変更することが極く一般的に行われている。

このようなデバイスドライバに再暗号／再復号処理及び鍵の管理機能を組み込むこととによりオペレーションシステムのカーネル部にこれらの機能を容易に組み込むことができる。また、固定鍵 K0 を用いて再暗号化する前に第 2 可変鍵 K2 を用いて再暗号化することにより、もし固定鍵 K0 が知られてしまった場合でもデータは第 2 可変鍵 K2 でも暗号化されているため、第 2 可変鍵 K2 を見いだして暗号化データの解読を行うことは極めて困難になる。

また、第 2 可変鍵 K2 は初めに使用され、固定鍵 K0 が使用された後に、最後に使用されるため、鍵の安全性が高く、かつ初めに使用されることにより、暗号化データを最も強力に支配することになる。

第 2 可変鍵 K2 は何度も繰り返して使用されると知られてしまう危険性がある。

専用の装置で利用される場合には許されない保存、複写あるいは転送を防止することは比較的容易に実現することができる。また、著作権主張がなされ暗号化されたデジタルデータがコンピュータにおいて利用される場合には、特開平 8-287014 (USP5867579, EP0715241A2) に示された復号／再暗号化用装置あるいは USP 5805706 に示された復号／再暗号化用装置を用いることにより、復号化されたデジタルデータを保存、複写あるいは転送を管理することが可能である。

しかしながら、コンピュータのバス上には表示あるいは印刷のために復号化されたデジタルデータが存在しており、バスに接続された装置を経由して復号化されたデジタルデータを保存、複写あるいは転送することが可能である。この問題を防止することができる著作権管理装置を説明する。

第 12 図に示されたのは著作権管理装置の構成例であり、この著作権管理装置では暗号鍵は第 1 可変鍵及び第 2 可変鍵が用いられる。

また、著作権管理装置は安全のためサブボード、PCMCIA カード、IC カードあるいは IC パッケージの形態で実現される。

この図において、101 は CPU であり、CPU 101 に接続されたシステムバス 102 に ROM 103, RAM 104, ハードディスクドライブ 105, フレキシブルディスクドライブ 105, CD-ROM ドライブ 107 及びモデム 108 等が接続されている。

109 は著作権管理装置であり、著作権管理装置 109 は復号化／暗号化ユニット 110 及びビデオインターフェース 113, オーディオインターフェース 114, プリンタインターフェース 115 を有している。

ビデオインターフェース 113, オーディオインターフェース 114, プリンタインターフェース 115 にはコンピュータの外部に各々表示装置 116, スピーカ 117 及びプリンタ 118 が接続される。

復号化／暗号化ユニット 110 は復号化ユニット 111 及び暗号化ユニット 112 を有している。

復号化／暗号化ユニット 110 の復号化ユニット 111 及び暗号化ユニット 1

データ著作権管理装置 109 の外には存在しない。

コンピュータ内には復号化デジタルデータの他に、暗号化されていないデジタルデータも存在する。

このような非暗号化デジタルデータと復号化データを区別して処理するためにはビデオインターフェース、オーディオインターフェース及びプリンタインターフェースを別に設けなければならず、装置が複雑高価になる。このようなことを避けるために、著作権管理装置 109 のビデオインターフェース 113、オーディオインターフェース 114 で非暗号化デジタルデータを処理するようにすることもできる。

第 13 図に示されたのは著作権管理装置の他の構成例であり、この著作権管理装置では暗号鍵は第 1 可変鍵及び第 2 可変鍵に加えて固定鍵が用いられる。

また、著作権管理装置は安全のためサブボード、PCMCIA カード、IC カードあるいは IC パッケージの形態で実現される。

この図において、101 は CPU であり、CPU 101 に接続されたシステムバス 102 に ROM 103、RAM 104、ハードディスクドライブ 105、フレキシブルディスクドライブ 105、CD-ROM ドライブ 107 及びモデム 108 等が接続されている。

120 は著作権管理装置であり、著作権管理装置 120 は復号化／暗号化ユニット 110 に加えて固定鍵暗号化ユニット 121 及び暗号化ビデオインターフェース 122、暗号化オーディオインターフェース 123、暗号化プリンタインターフェース 124 を有している。

復号化／再暗号化ユニット 110 は復号化ユニット 111 及び暗号化ユニット 112 を有している。

また、暗号化ビデオインターフェース 122、暗号化オーディオインターフェース 123、暗号化プリンタインターフェース 124 にコンピュータの外部の暗号化デジタル画像表示装置 125、暗号化デジタル音声再生装置 126 及び暗号化デジタルプリンタ 127 が接続される。

復号化デジタルデータMがハードディスクドライブ105で保存、フレキシブルディスクドライブ105で複写あるいはモデム108を経由して転送される場合には、再暗号ユニット115において第2可変鍵K2を用いて再暗号化され、

$$\forall 2: C2 = E(M, K2)$$

$$= E(D(C1, K1), K2)$$

再暗号化デジタルデータC2がシステムバス102に供給され、ハードディスクドライブ105で保存、フレキシブルディスクドライブ105で複写あるいはモデム108を経由して転送される。

復号化デジタルデータMが暗号化データ表示装置125、暗号化データ音声装置126又は暗号化データプリンタ127に出力される場合は著作権管理装置120内の固定鍵暗号化ユニット121において固定鍵K0を用いて再暗号化され、

$$\forall 0: C0 = E(M, K0)$$

$$= E(D(C1, K1), K0)$$

再暗号化デジタルデータC0が暗号化ビデオインターフェース122、暗号化オーディオインターフェース123及びプリンタインターフェース124において暗号化データ表示装置125、暗号化データ音声装置126又は暗号化データプリンタ127にそれぞれ適合するように編成され、暗号化表示信号Cd0、暗号化音声信号Ca0及び暗号化プリンタ信号Cp0として出力される。

暗号化ビデオインターフェース122から暗号化データ表示装置125に入力された暗号化表示信号Cd0は固定鍵復号化装置128において、固定鍵K0を用いて復号化され、

$$Md = D(Cd0, K0)$$

復号化表示信号MdがD/A変換器131において表示可能なアナログ信号とされ、表示装置116に表示される。

なお、この場合表示装置116がデジタルデータをそのまま表示可能なデジタル表示装置である場合にはD/A変換器131は不要である。

この図において、101はCPUであり、CPU101に接続されたシステムバス102にROM103、RAM104、ハードディスクドライブ105、フレキシブルディスクドライブ105、CD-ROMドライブ107及びモデム108等が接続されている。

140は著作権管理装置であり、著作権管理装置140は復号化／再暗号化ユニット110、ビデオインターフェース131、オーディオインターフェース132、プリンタインターフェース133及び固定鍵暗号化ユニット134を有している。

復号化／再暗号化ユニット110は復号化ユニット111及び再暗号化ユニット112を有している。

また、固定鍵暗号化ユニット134はビデオ用固定鍵暗号化ユニット142135、オーディオ用固定鍵暗号化ユニット136及びプリンタ用固定鍵暗号化ユニット137を有しているが、これらのビデオ用固定鍵暗号化ユニット135、オーディオ用固定鍵暗号化ユニット136及びプリンタ用固定鍵暗号化ユニット137は暗号化能力が十分であれば単一であることも可能である。

復号化／再暗号化ユニット110の復号化ユニット111及び再暗号化ユニット112はともにコンピュータのシステムバス102に接続され、復号化ユニット111にはさらにビデオインターフェース113、オーディオインターフェース114及びプリンタインターフェース115が接続され、これらのインターフェースにビデオ用固定鍵暗号化ユニット135、オーディオ用固定鍵暗号化ユニット136及びプリンタ用固定鍵暗号化ユニット137が接続されている。

ビデオ用固定鍵暗号化ユニット135、オーディオ用固定鍵暗号化ユニット136及びプリンタ用固定鍵暗号化ユニット137にはコンピュータの外部の暗号化デジタル画像表示装置125、暗号化デジタル音声再生装置126及び暗号化デジタルプリンタ127が接続される。

このような構成は著作権管理装置120はCPUとシステムバスを有するサブコンピュータ構成とすることにより容易に実現することができる。

暗号化データ表示装置125はビデオ用固定鍵暗号化ユニット135に接続さ

々表示装置 1 1 6, 音声装置 1 1 7 及びプリンタ 1 1 8 に適合するデジタルデータ Md, Ma 及び Mp に編成され、これらのデジタルデータが各々表示用固定鍵暗号化ユニット 1 3 5, 音声用固定鍵暗号化ユニット 1 3 6 及びプリンタ用固定鍵暗号化ユニット 1 3 7 において固定鍵 K0 を用いて暗号化され、

$$Cd0 = E(Md, K0)$$

$$Ca0 = E(Ma, K0)$$

$$Cp0 = E(Mp, K0)$$

暗号化表示信号 Cd0, 暗号化音声信号 Ca0 及び暗号化プリンタ信号 Cp0 として出力される。

表示用固定鍵暗号化ユニット 1 3 5 から暗号化データ表示装置 1 2 5 に入力された暗号化表示信号 Cd0 は固定鍵復号化装置 1 2 8 において、固定鍵 K0 を用いて復号化され、

$$Md = D(Cd0, K0)$$

復号化表示信号 Md が D/A 変換器 1 3 1 において表示可能なアナログ信号とされ、表示装置 1 1 6 に表示される。

なお、この場合表示装置 1 1 6 がデジタルデータをそのまま表示可能なデジタル表示装置である場合には D/A 変換器 1 3 1 は不要である。

音声用固定鍵暗号化ユニット 1 3 6 から暗号化データ音声装置 1 2 6 に入力された暗号化音声信号 Ca0 は固定鍵復号化装置 1 2 9 において、固定鍵 K0 を用いて復号化され、

$$Ma = D(Ca0, K0)$$

復号化音声信号 Ma が D/A 変換器 1 3 2 において表示可能なアナログ信号とされ、スピーカ 1 1 6 で再生される。

プリンタ用固定鍵暗号化ユニット 1 3 7 から暗号化データプリンタ 1 2 7 に入力された暗号化プリンタ信号 Cp0 は固定鍵復号化装置 1 3 0 において、固定鍵 K0 を用いて復号化され、

請 求 の 範 囲

1 暗号化デジタルデータから復号化された復号化デジタルデータを不正な利用から保護するデジタルデータ保護方法であって：前記デジタルデータ保護方法は、

前記復号化デジタルデータを可変鍵を用いて暗号化して可変鍵再暗号化デジタルデータとする過程；

前記可変鍵再暗号化デジタルデータを保存、複写又は転送するために使用装置に内蔵されている固定鍵を用いて暗号化して固定鍵－可変鍵 2 重再暗号化デジタルデータとする過程；

保存、複写又は転送された前記固定鍵－可変鍵 2 重再暗号化デジタルデータを前記固定鍵を用いて復号化して可変鍵再暗号化デジタルデータとする過程；

前記可変鍵再暗号化デジタルデータを前記可変鍵を用いて復号化して前記復号化デジタルデータとする過程；

を有する。

2 暗号化デジタルデータから復号化された復号化デジタルデータを不正な利用から保護するデジタルデータ保護方法であって：前記デジタルデータ保護方法は、

前記復号化デジタルデータを使用装置に内蔵されている固定鍵を用いて暗号化して固定鍵再暗号化デジタルデータとする過程；

前記固定鍵再暗号化デジタルデータを保存、複写又は転送するために前記固定鍵再暗号化デジタルデータを可変鍵を用いて暗号化して固定鍵－可変鍵 2 重再暗号化デジタルデータとする過程；

保存、複写又は転送された前記固定鍵－可変鍵 2 重再暗号化デジタルデータを前記可変鍵を用いて復号化して可変鍵再暗号化デジタルデータとする過程；

前記可変鍵再復号化デジタルデータを前記固定鍵を用いて復号化して前記復号化デジタルデータとする過程；

を有する。

3 前記可変鍵を用いての暗号化及び復号化がソフトウェアによって行われる；

前記可変鍵再暗号化デジタルデータを保存、複写又は転送するために使用装置に内蔵されている固定鍵を用いて再暗号化して可変鍵－固定鍵 2 重再暗号化デジタルデータとする固定鍵暗号化ユニット；

保存、複写又は転送された可変鍵－固定鍵 2 重再暗号化デジタルデータを前記固定鍵を用いて復号化して固定鍵再暗号化デジタルデータとする固定鍵復号化ユニット；

前記固定鍵再暗号化デジタルデータを前記可変鍵を用いて復号化して前記復号化デジタルデータとする可変鍵復号化ユニット；

を有する。

1 5 暗号化デジタルデータから復号化された復号化デジタルデータを不正な利用から保護するデジタルデータ保護装置であって：前記デジタルデータ保護装置は、

前記復号化デジタルデータを使用装置に内蔵されている固定鍵を用いて再暗号化して固定鍵再暗号化デジタルデータとする固定鍵暗号化ユニット；

前記固定鍵再暗号化デジタルデータを保存、複写又は転送するために可変鍵を用いて暗号化して可変鍵－固定鍵 2 重再暗号化デジタルデータとする可変鍵暗号化ユニット；

保存、複写又は転送された可変鍵－固定鍵 2 重再暗号化デジタルデータを可変鍵を用いて復号化して固定鍵再暗号化デジタルデータとする可変鍵復号化ユニット；

前記固定鍵再暗号化デジタルデータを前記固定鍵を用いて復号化して前記復号化デジタルデータとする固定鍵復号化ユニット；

を有する。

1 6 前記可変鍵を用いての暗号化及び復号化がソフトウェアによって行われる：

請求の範囲 1 4 又は請求の範囲 1 5 のデジタルデータ保護装置。

1 7 前記可変鍵を用いての暗号化及び復号化がハードウェアによって行われる：

請求の範囲 1 4 又は請求の範囲 1 5 のデジタルデータ保護装置。

を用いて復号化して前記第 2 可変鍵再暗号化デジタルデータとする過程；

前記第 2 可変鍵再暗号化デジタルデータを複写又は転送するために第 3 可変鍵を用いて暗号化して第 3 可変鍵－第 2 可変鍵 2 重再暗号化デジタルデータとする過程；

複写又は転送された前記第 3 可変鍵－第 2 可変鍵 2 重再暗号化デジタルデータを前記第 3 可変鍵を用いて復号化して第 2 可変鍵再暗号化デジタルデータとする過程；

前記第 2 可変鍵再暗号化デジタルデータを前記第 2 可変鍵を用いて復号化して復号化デジタルデータとする過程；

を有する。

28 第 1 可変鍵暗号化デジタルデータから復号化された復号化デジタルデータを不正な利用から保護するデジタルデータ保護方法であって：前記デジタルデータ保護方法は、

前記復号化デジタルデータを第 2 可変鍵を用いて暗号化して第 2 可変鍵再暗号化デジタルデータとする過程；

前記第 2 可変鍵再暗号化デジタルデータを保存するために使用装置に内蔵されている固定鍵を用いて暗号化して固定鍵－第 2 可変鍵 2 重再暗号化デジタルデータとする過程；

保存された前記固定鍵－第 2 可変鍵 2 重再暗号化デジタルデータを前記固定鍵を用いて復号化して前記第 2 可変鍵再暗号化デジタルデータとする過程；

前記第 2 可変鍵再暗号化デジタルデータを複写又は転送するために第 3 可変鍵を用いて暗号化して第 3 可変鍵－第 2 可変鍵 2 重再暗号化デジタルデータとする過程；

複写又は転送された前記第 3 可変鍵－第 2 可変鍵 2 重再暗号化デジタルデータを前記第 3 可変鍵を用いて復号化して第 2 可変鍵再暗号化デジタルデータとする過程；

前記第 2 可変鍵再暗号化デジタルデータを前記第 2 可変鍵を用いて復号化して復号化デジタルデータとする過程；

を有する。

変鍵を用いて復号化して固定鍵再暗号化デジタルデータとする過程；

前記固定鍵再暗号化デジタルデータを前記固定鍵を用いて復号化して復号化デジタルデータとする過程；

前記再暗号化デジタルデータを複写又は転送するために第3可変鍵を用いて暗号化して第3可変鍵再暗号化デジタルデータとし、前記第3可変鍵再暗号化デジタルデータを前記第2可変鍵を用いて暗号化して第2可変鍵—第3可変鍵2重再暗号化デジタルデータとする過程；

複写又は転送された第2可変鍵—第3可変鍵2重再暗号化デジタルデータを前記第2可変鍵を用いて復号化して第3可変鍵再暗号化デジタルデータとする過程；

前記第3可変鍵再暗号化デジタルデータを前記第3可変鍵を用いて復号化して復号化デジタルデータとする過程；

を有する。

3 1 前記第2可変鍵を用いての暗号化及び復号化がソフトウェアによって行われる：

請求の範囲27，請求の範囲28，請求の範囲29又は請求の範囲30のデジタルデータ保護方法。

3 2 前記第2可変鍵を用いての暗号化及び復号化がハードウェアによって行われる：

請求の範囲27，請求の範囲28，請求の範囲29又は請求の範囲30のデジタルデータ保護方法。

3 3 前記第2可変鍵が外部から供給される：

請求の範囲27，請求の範囲28，請求の範囲29又は請求の範囲30のデジタルデータ保護方法。

3 4 前記第2可変鍵が使用装置の内部で生成される：

請求の範囲27，請求の範囲28，請求の範囲29又は請求の範囲30のデジタルデータ保護方法。

3 5 前記第3可変鍵を用いての暗号化及び復号化がソフトウェアによって行われる：

4 4 前記固定鍵が前記使用装置に固有である；

請求の範囲 4 1，請求の範囲 4 2 又は請求の範囲 4 3 のデジタルデータ保護方法。

4 5 前記固定鍵が前記使用装置に固有ではない；

請求の範囲 4 1，請求の範囲 4 2 又は請求の範囲 4 3 のデジタルデータ保護方法。

4 6 第 1 可変鍵暗号化デジタルデータから復号化された復号化デジタルデータを不正な利用から保護するデジタルデータ保護装置であって：前記デジタルデータ保護装置は、

前記復号化デジタルデータを第 2 可変鍵を用いて暗号化して第 2 可変鍵再暗号化デジタルデータとする第 2 可変鍵暗号化ユニット；

前記第 2 可変鍵再暗号化デジタルデータを保存するために使用装置に内蔵されている固定鍵を用いて暗号化して固定鍵—第 2 可変鍵 2 重再暗号化デジタルデータとする固定鍵暗号化ユニット；

保存された前記固定鍵—第 2 可変鍵 2 重再暗号化デジタルデータを前記固定鍵を用いて復号化して前記第 2 可変鍵再暗号化デジタルデータとする固定鍵復号化ユニット；

前記第 2 可変鍵再暗号化デジタルデータを複写又は転送するために第 3 可変鍵を用いて暗号化して第 3 可変鍵—第 2 可変鍵 2 重再暗号化デジタルデータとする第 3 可変鍵暗号化ユニット；

複写又は転送された前記第 3 可変鍵—第 2 可変鍵 2 重再暗号化デジタルデータを前記第 3 可変鍵を用いて復号化して第 2 可変鍵再暗号化デジタルデータとする第 3 可変鍵復号化ユニット；

復号化された前記第 2 可変鍵再暗号化デジタルデータを前記第 2 可変鍵を用いて復号化して復号化デジタルデータとする第 2 可変鍵復号化ユニット；

を有する。

4 7 第 1 可変鍵暗号化デジタルデータから復号化された復号化デジタルデータを不正な利用から保護するデジタルデータ保護装置であって：前記デジタルデータ保護装置は、

前記復号化デジタルデータを第 2 可変鍵を用いて暗号化して第 2 可変鍵再暗号

び前記第 3 可変鍵再暗号化デジタルデータを前記第 2 可変鍵を用いて暗号化して第 2 可変鍵—第 3 可変鍵 2 重再暗号化デジタルデータとする第 2 可変鍵暗号化ユニット；

複写又は転送された第 2 可変鍵—第 3 可変鍵 2 重再暗号化デジタルデータを前記第 2 可変鍵を用いて復号化して第 3 可変鍵再暗号化デジタルデータとする第 2 可変鍵復号化ユニット及び前記第 3 可変鍵再暗号化デジタルデータを前記第 3 可変鍵を用いて復号化して復号化デジタルデータとする第 3 可変鍵復号化ユニット；

を有する。

49 第 1 可変鍵暗号化デジタルデータから復号化された復号化デジタルデータを不正な利用から保護するデジタルデータ保護装置であって：前記デジタルデータ保護装置は、

前記復号化デジタルデータを保存するために使用装置に内蔵されている固定鍵を用いて暗号化して固定鍵再暗号化デジタルデータとする固定鍵暗号化ユニット及び前記固定鍵再暗号化デジタルデータを第 2 可変鍵を用いて暗号化して第 2 可変鍵—固定鍵 2 重再暗号化デジタルデータとする第 2 可変鍵暗号化ユニット；

保存された前記第 2 可変鍵—固定鍵 2 重再暗号化デジタルデータを前記第 2 可変鍵を用いて復号化して固定鍵再暗号化デジタルデータとする第 2 可変鍵復号化ユニット及び前記固定鍵再暗号化デジタルデータを前記固定鍵を用いて復号化して復号化デジタルデータとする固定鍵復号化ユニット；

前記再暗号化デジタルデータを複写又は転送するために第 3 可変鍵を用いて暗号化して第 3 可変鍵再暗号化デジタルデータとする第 3 可変鍵暗号化ユニット及び前記第 3 可変鍵再暗号化デジタルデータを前記第 2 可変鍵を用いて暗号化して第 2 可変鍵—第 3 可変鍵 2 重再暗号化デジタルデータとする第 2 可変鍵暗号化ユニット；

複写又は転送された第 2 可変鍵—第 3 可変鍵 2 重再暗号化デジタルデータを前記第 2 可変鍵を用いて復号化して第 3 可変鍵再暗号化デジタルデータとする第 2 可変鍵復号化ユニット及び前記第 3 可変鍵再暗号化デジタルデータを前記第 3 可変鍵を用いて復号化して復号化デジタルデータとする第 3 可変鍵復号化ユニット

タルデータ保護装置。

5 8 前記固定鍵を用いての暗号化及び復号化がソフトウェアによって行われる：

請求の範囲 4 6，請求の範囲 4 7，請求の範囲 4 8 又は請求の範囲 4 9 のデジタルデータ保護装置。

5 9 前記固定鍵を用いての暗号化及び復号化がハードウェアによって行われる：

請求の範囲 4 6，請求の範囲 4 7，請求の範囲 4 8 又は請求の範囲 4 9 のデジタルデータ保護装置。

6 0 前記固定鍵が前記使用装置に当初から内蔵されている；

請求の範囲 4 6，請求の範囲 4 7，請求の範囲 4 8 又は請求の範囲 4 9 のデジタルデータ保護装置。

6 1 前記固定鍵が使用装置の内部で生成される；

請求の範囲 4 6，請求の範囲 4 7，請求の範囲 4 8 又は請求の範囲 4 9 のデジタルデータ保護装置。

6 2 前記固定鍵が使用装置の外部から供給される；

請求の範囲 4 6，請求の範囲 4 7，請求の範囲 4 8 又は請求の範囲 4 9 のデジタルデータ保護装置。

6 3 前記固定鍵が前記使用装置に固有である；

請求の範囲 6 0，請求の範囲 6 1 又は請求の範囲 6 2 のデジタルデータ保護装置。

6 4 前記固定鍵が前記使用装置に固有ではない；

請求の範囲 6 0，請求の範囲 6 1 又は請求の範囲 6 2 のデジタルデータ保護装置。

6 5 デジタルデータを不正な利用から保護するデジタルデータ保護方法であって：前記デジタルデータ保護方法は、

前記デジタルデータが保護対象であるか否かを判定する過程；

保護対象であると判定された前記デジタルデータを前記使用装置に内蔵されている固定鍵を用いて暗号化して固定鍵暗号化デジタルデータとする過程；

7 5 前記固定鍵が前記使用装置に固有ではない；

請求の範囲 7 1，請求の範囲 7 2 又は請求の範囲 7 3 のデジタルデータ保護装置。

7 6 デジタルデータを不正な利用から保護するデジタルデータ保護装置であって：前記デジタルデータ保護装置は、

前記デジタルデータが保護対象であるか否かを判定する過程；

保護対象であると判定された前記デジタルデータを前記使用装置に内蔵されている固定鍵を用いて暗号化して固定鍵暗号化デジタルデータとする過程；

保護対象であると判定されなかった前記デジタルデータ及び前記固定鍵暗号化デジタルデータを保存、複写又は転送する過程；

保存、複写又は転送された前記固定鍵暗号化デジタルデータを前記固定鍵を用いて復号化して復号化デジタルデータとする過程；

保存、複写又は転送された前記デジタルデータ及び前記復号化デジタルデータを利用する過程；

を有する。

7 7 前記固定鍵を用いての暗号化及び復号化がソフトウェアによって行われる：

請求の範囲 7 6 のデジタルデータ保護装置。

7 8 前記固定鍵を用いての暗号化及び復号化がハードウェアによって行われる：

請求の範囲 7 6 のデジタルデータ保護装置。

7 9 前記固定鍵を用いての暗号化及び復号化が前記デジタルデータに付加された識別符号によって制御される：

請求の範囲 7 6 のデジタルデータ保護装置。

8 0 暗号化及び復号化が前記識別符号があることにより行われる：

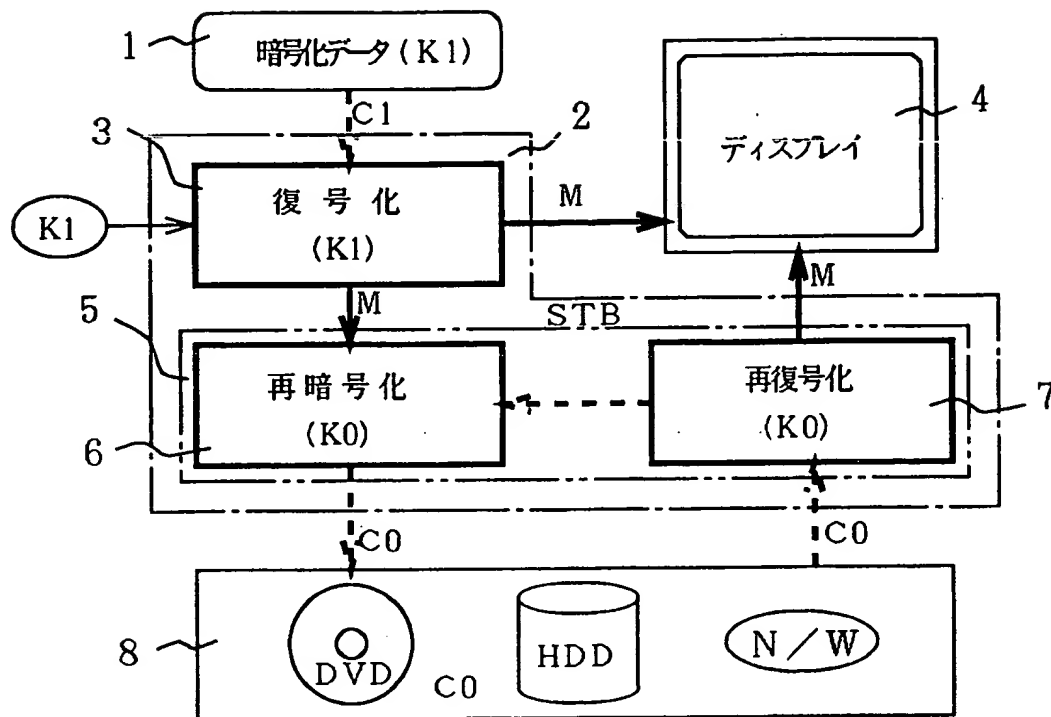
請求の範囲 7 6 のデジタルデータ保護装置。

8 1 暗号化及び復号化が前記識別符号がないことにより行われる：

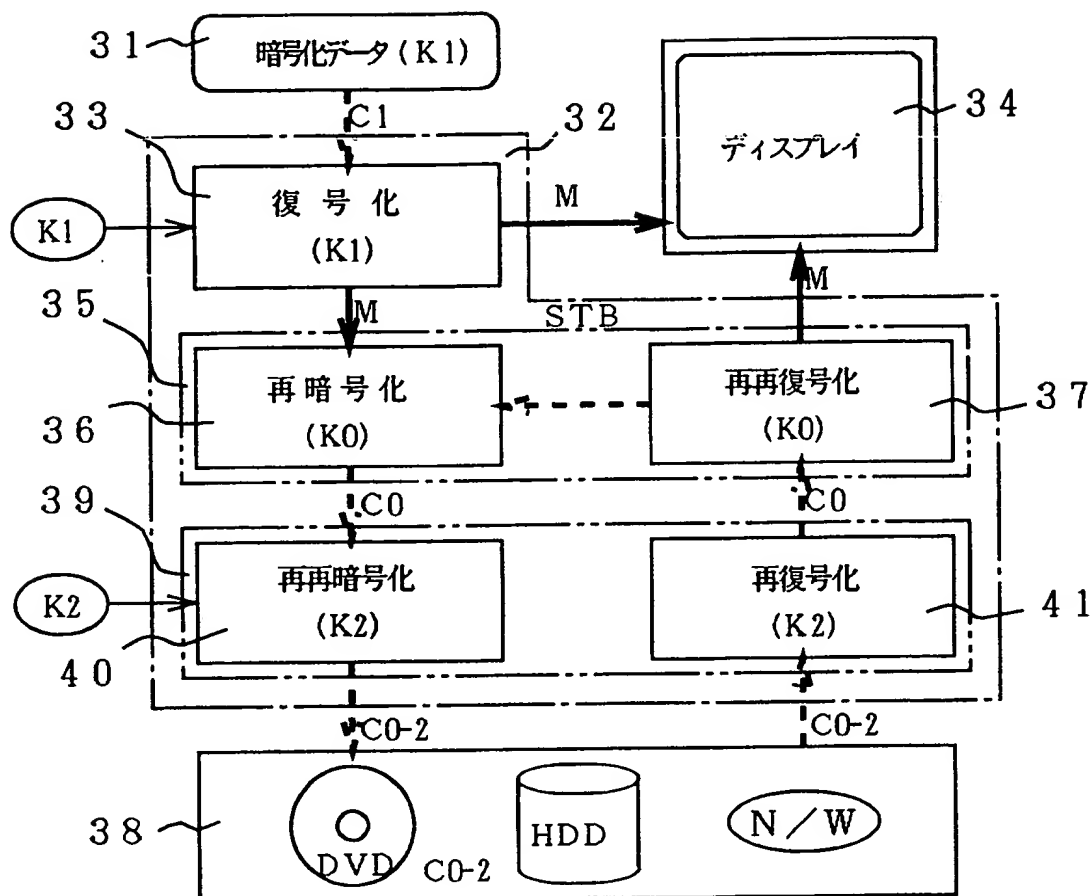
請求の範囲 7 6 のデジタルデータ保護装置。

8 2 前記固定鍵が使用装置に当初から内蔵されている；

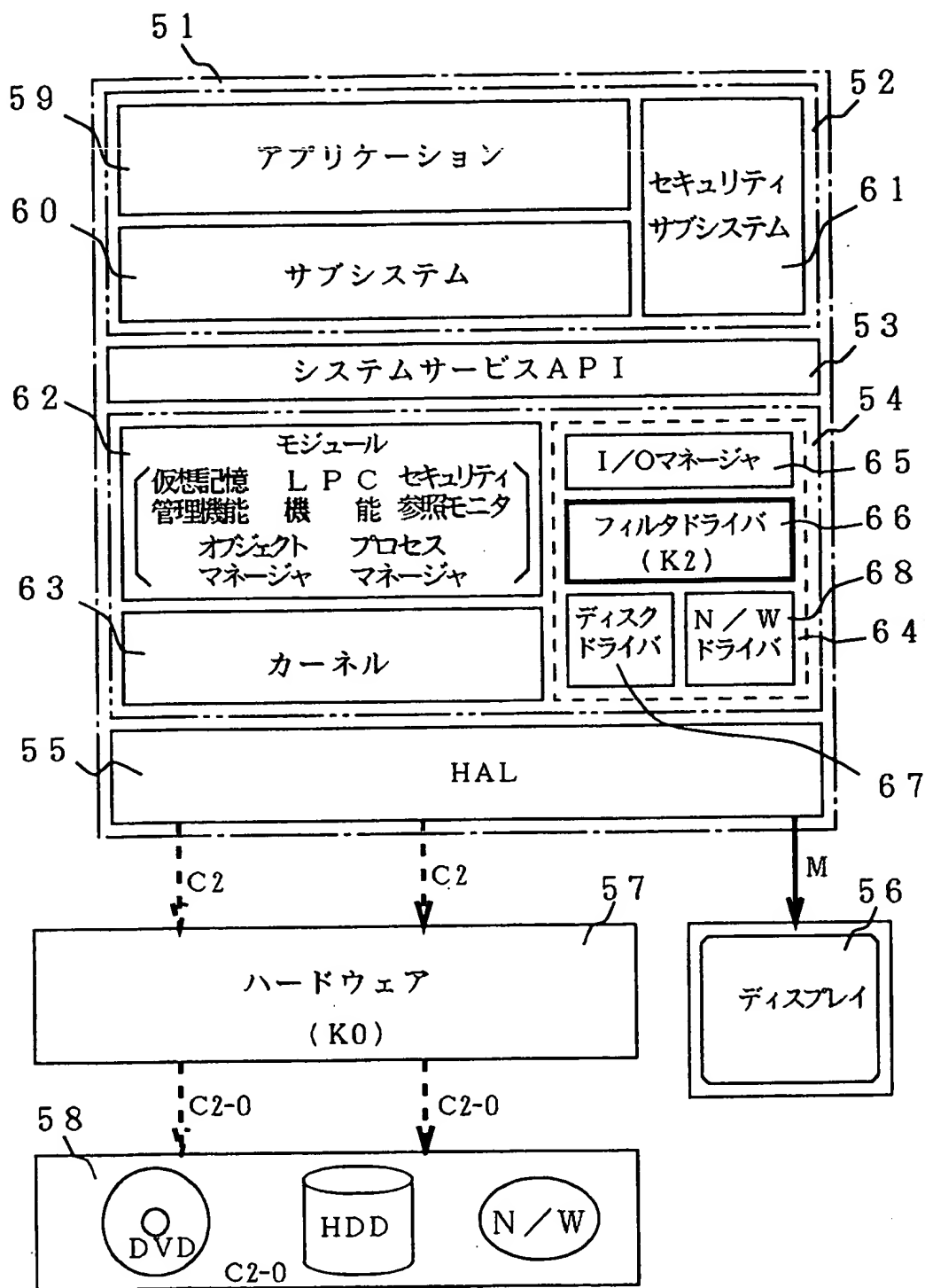
第1図



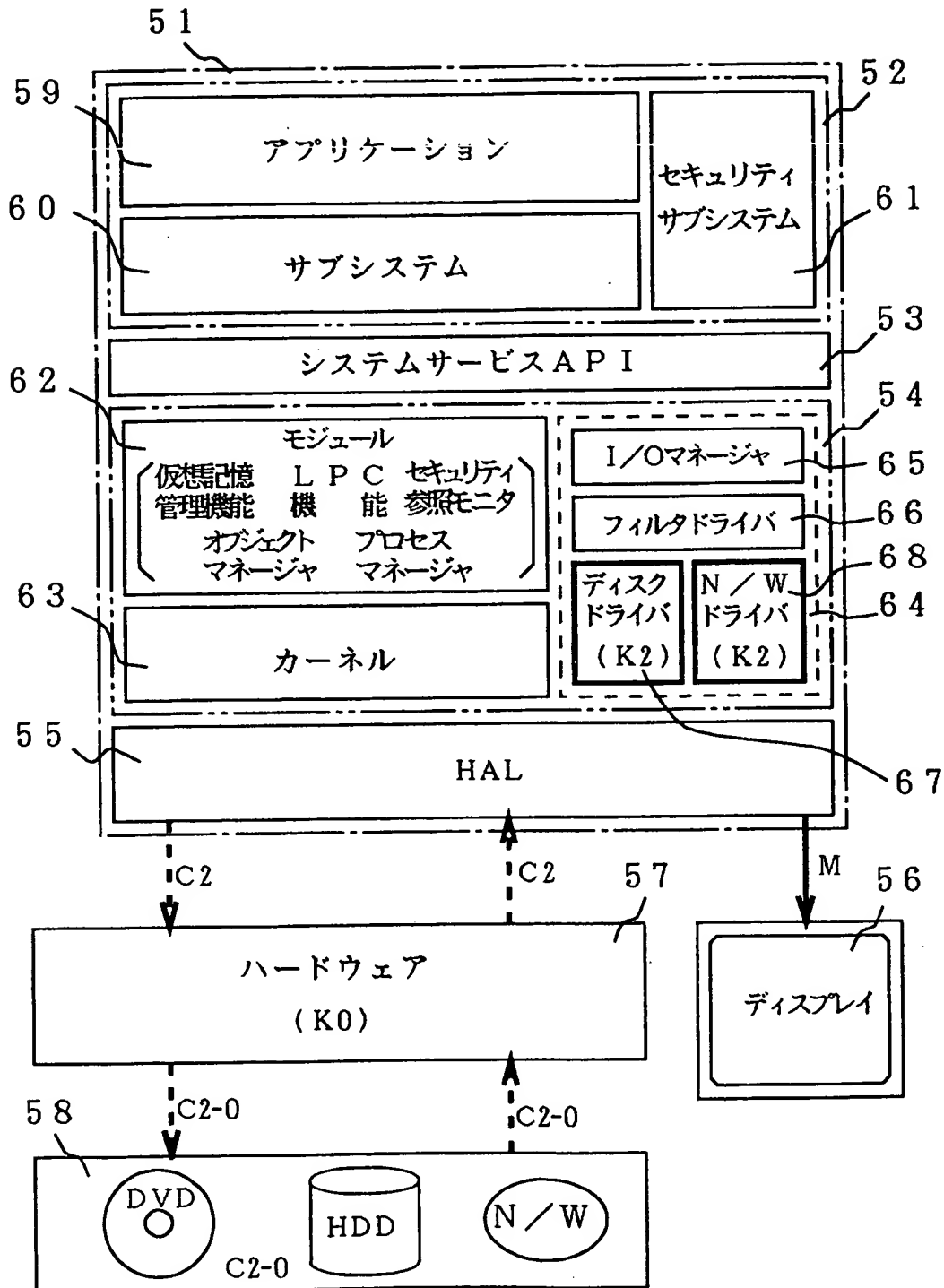
第3図



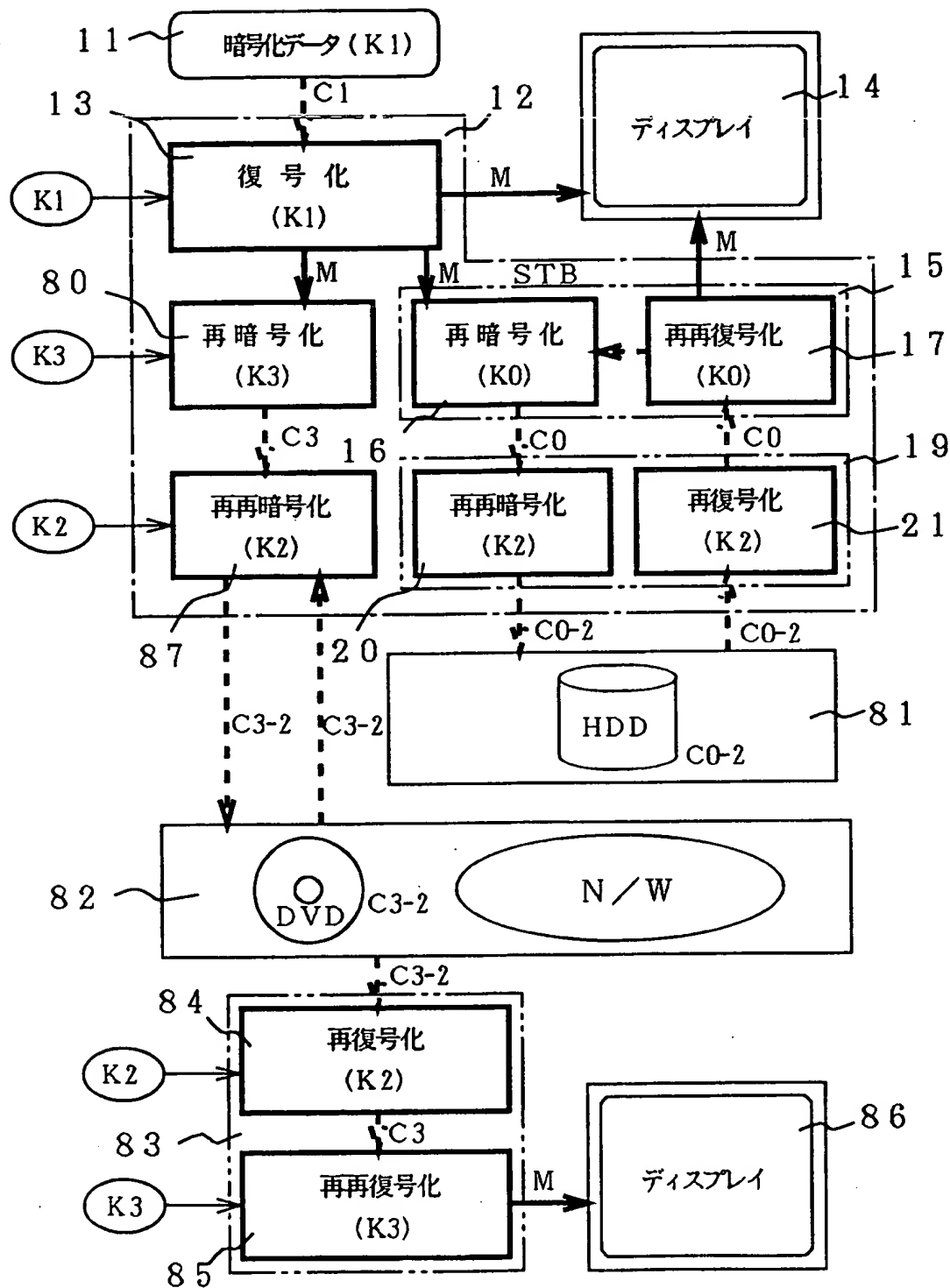
第5図



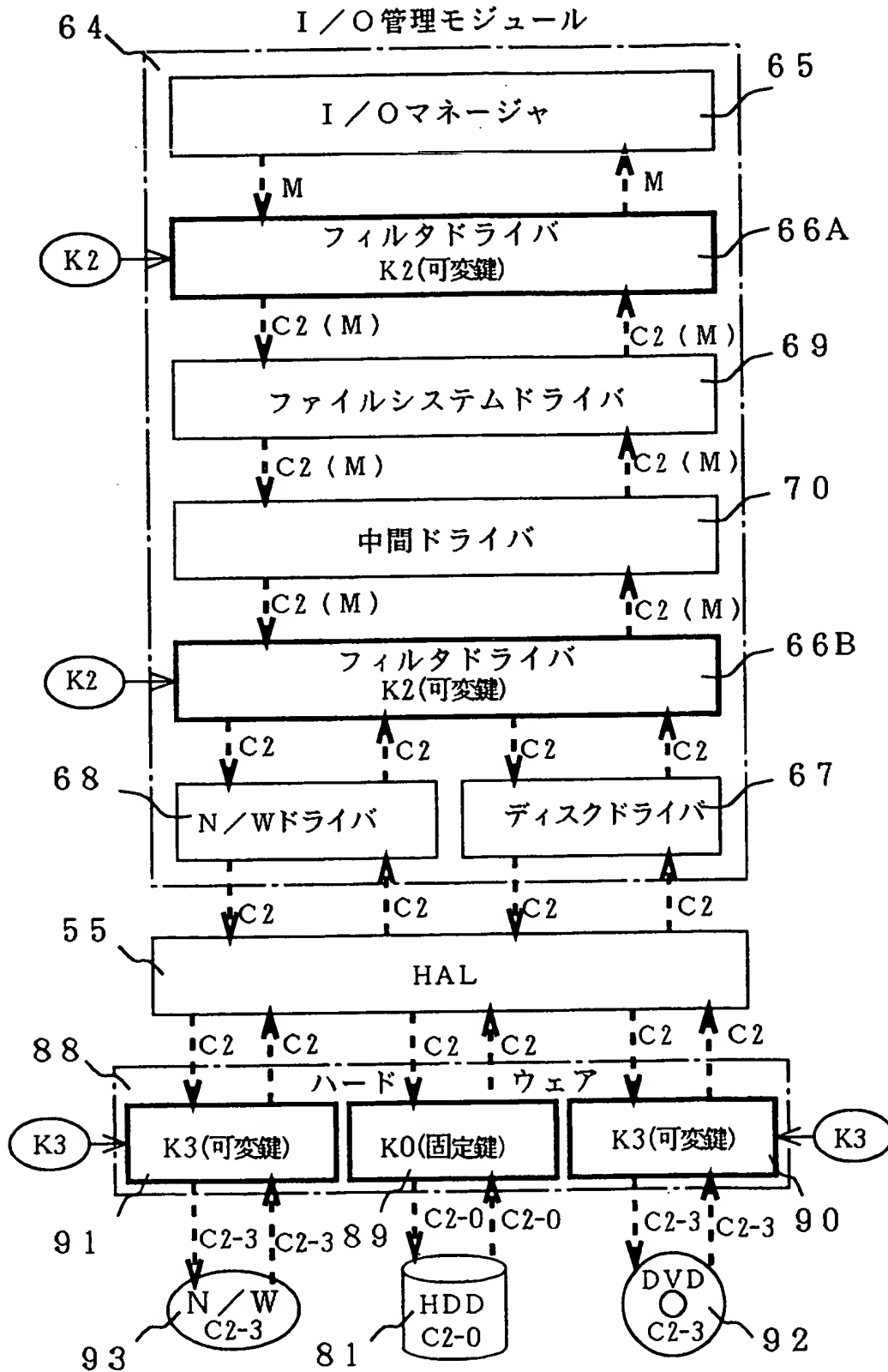
第7図



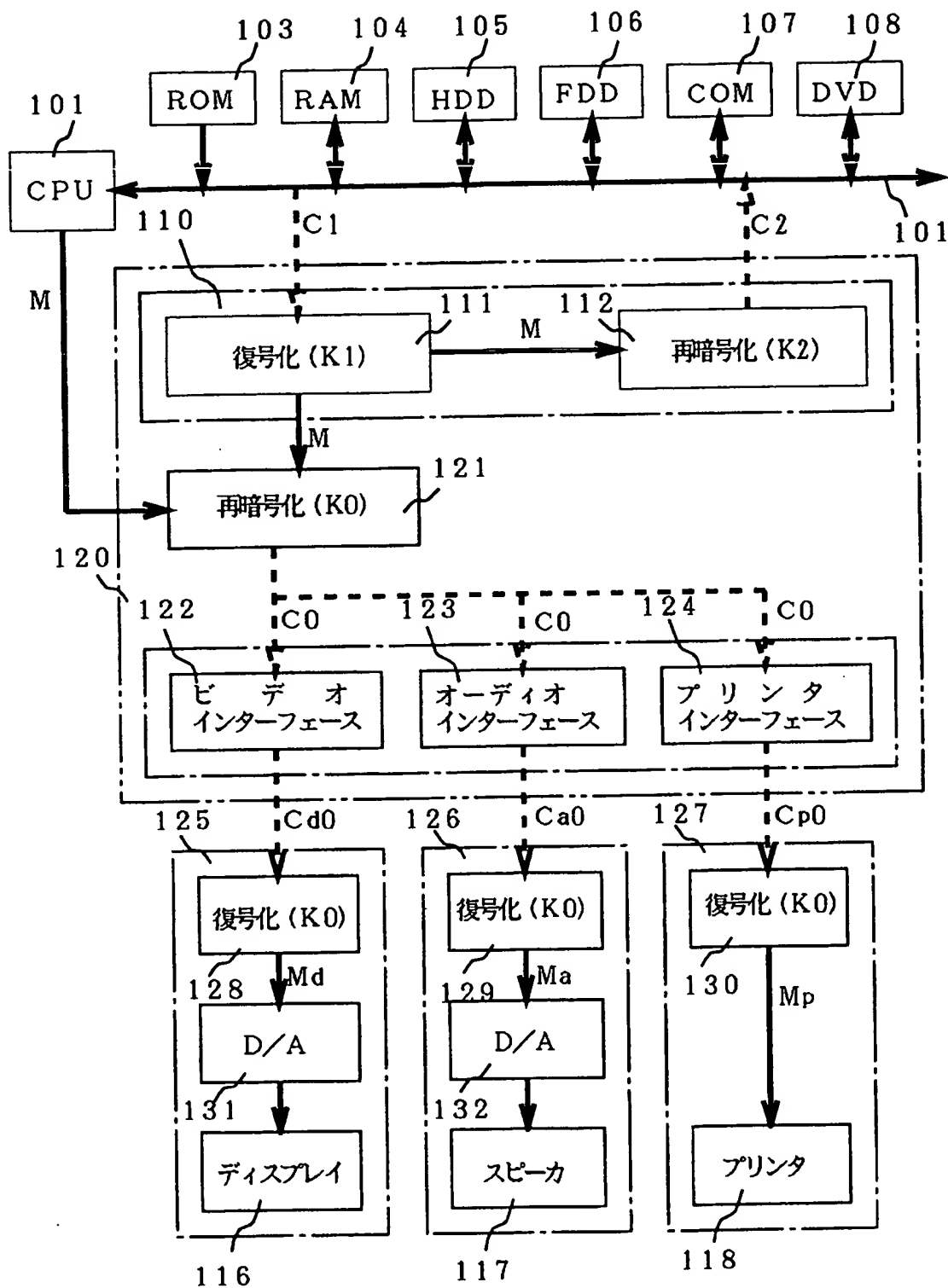
第9図



第11図



第13図



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP99/05704

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ H04L 9/14 G11B 20/10 H04N 7/167 G06F 17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ H04L 9/00-9/38 H04K 1/00-3/00 G09C 1/00-5/00
G11B 20/10 H04N 7/167

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JICST (JOIS)
INSPEC (DIALOG)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	"Make a dash for universalization by overcoming 4 problems", Nikkei Electronics, No. 724, (24 August, 1998), pages 101-111; especially, page 109, right column to page 111	1-86
Y	Bruce Schneier, APPLIED CRYPTOGRAPHY, second edition, John Wiley & Sons, (1996), pages 357-368, Especially, pages 357, 358, 367, 368	1-64
PX	JP, 11-275516, A (Hitachi, Ltd.), 08 October, 1999 (08.10.99) (Family: none)	65-86
Y	JP, 7-272399, A (Hitachi, Ltd.), 20 October, 1995 (20.10.95) & US, 5912969, A	1, 2, 14, 15, 27-30, 46-49, 65, 76
Y	Shoji Miyaguchi, Akira Shiraishi and Akihiro Shimizu, "Fast Data Encipherment Algorithm FEAL-8," REVIEW of the Electrical Communications Laboratories, Vol. 36, No. 4, (1988), pages 433-437, especially, page 433, left column	3, 7, 16, 20, 31, 35, 39, 50, 54 , 58, 66, 77

☒ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
13 January, 2000 (13.01.00)Date of mailing of the international search report
25 January, 2000 (25.01.00)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP99/05704

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The subject matter of claims 1 to 64 relates to an idea of doubly encrypting digital data using different keys and then storing, copying, and transferring the encrypted data. The subject matter of claims 65 to 86 relates to an idea of encrypting digital data to be protected, and storing, copying, and transferring the other digital data without encrypting it. Therefore, the requirement of unity of invention is not satisfied.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐

The additional search fees were accompanied by the applicant's protest.

☒

No protest accompanied the payment of additional search fees.

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	J P, 7-272399, A (株式会社日立製作所) 20. 10月. 1995 (20. 10. 95) & US, 5912969, A	1, 2, 14, 15, 27-30, 46-49, 65, 76
Y	Shoji Miyaguchi, Akira Shiraishi and Akihiro Shimizu, "Fast Data Encipherment Algorithm FEAL-8," REVIEW of the Electrical Communications Laboratories, Vol. 36, No. 4, (1988), pp. 433-437 特に第433頁左欄参照	3, 7, 16, 20, 31, 35, 39, 50, 54, 58, 66, 77
Y	小柳津育郎, 松本博幸, 石井晋司 "マルチメディア通信用LSI" 情報処理学会研究報告, Vol. 91, No. 8 (DPS-48), (1991), pp. 73-80 特に第74頁左欄参照	4, 8, 17, 21, 32, 36, 40, 51, 55, 59, 67, 78
Y	J P, 8-185448, A (三菱商事株式会社) 16. 7月. 1996 (16. 07. 96) & EP, 704785, A2	5, 11, 18, 24, 33, 37, 43, 56, 62, 73, 84
Y	J P, 8-125651, A (株式会社日立製作所) 17. 5月. 1996 (17. 05. 96) (ファミリーなし)	6, 10, 19, 23, 34, 38, 42, 53, 57, 61, 72, 83
Y	J P, 10-271105, A (トムソン マルチメディア ソシエテ アノニム) 9. 10月. 1998 (09. 10. 98) & EP, 843438, A2 & FR, 2755809, A1 & ZA, 9710105, A & KR, 98042367, A	9, 12, 22, 25, 41, 44, 60, 63, 71, 74, 82, 85